I Claim:

1. A code inspection system comprising:

a code inspection management module that monitors and communicates with a protected system;

a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;

an actuator module; and

one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module.

2. The system of claim 1, wherein the actuator module at least one of executes the one or more portions of code, opens the one or more portions of code, inputs information to the one or more portions of code and simulates a passage of time longer than a period of testing.

3. The system of claim 1, wherein the one or more sensor modules detect one or more of unauthorized access attempts, unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine.

4. The system of claim 1, wherein the protected system is at least one of a computer, a plurality of computers, a network and one or more input devices.

5. The system of claim 1, wherein the dynamic decoy system can be incorporated into a portion of the protected system

6. The system of claim 5, wherein at least a portion of the code inspection system is in at least one of a BIOS and an operating system of the protected system.

7. The system of claim 1, wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

8. The system of claim 1, wherein at least a portion of the protected system is capable of being recovered from the dynamic decoy system.

9. The system of claim 1, wherein the code inspection management module monitors the protected system and updates the dynamic decoy system based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.

10. The system of claim 1, wherein the code inspection system is an interface between the protected system and one or more unprotected systems.

11. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system; and

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code.

12. The method of claim 11, wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

13. The method of claim 11, further comprising forwarding approved code to the protected system.

14. The method of claim 11, wherein the dynamic decoy system is an interface between the protected system and one or more unprotected systems.

15. The method of claim 11, further comprising restoring one or more portions of the protected system based on the dynamic decoy system

16. The method of claim 11, further comprising at least one of deleting and removing at least one unauthorized portion the one or more portions of code.

17. The method of claim 11, further comprising installing one or more sensors in the dynamic decoy system that detect one or more of unauthorized access attempts, unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine.

18. The method of claim 11, further comprising installing an actuator in the dynamic decoy system.

19. The method of claim 18, wherein the actuator at least one of executes the one or more portions of code, opens the one or more portions of code, inputs information to the one or more portions of code and simulates a passage of time longer than a period of testing.

20. The method of claim 11, wherein updating the dynamic decoy system is based on at least one of installed software, installed hardware, operating system

upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.

21. An information storage media comprising information that creates and maintains a dynamic decoy system based on a protected system comprising:

information that creates a dynamic decoy system that substantially parallels relevant portions of a protected system;

information that updates the dynamic decoy system based on changes to the protected system;

information that receives one or more portions of code;

information that introduces the one or more portions of code to the dynamic decoy system;

information that simulates operating conditions of the protected system in the dynamic decoy system; and

information that monitors sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code.

22. The media of claim 21, wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

23. The media of claim 21, further comprising information that forwards approved code to the protected system.

24. The media of claim 21, wherein the dynamic decoy system is an interface between the protected system and one or more unprotected systems.

25. The media of claim 21, further comprising information that restores one or more portions of the protected system based on the dynamic decoy system

26. The media of claim 21, further comprising information that at least one of deletes and removes at least one unauthorized portion of the one or more portions of code.

27. The media of claim 21, further comprising information that installs one or more sensors in the dynamic decoy system that detect one or more of unauthorized access attempts, unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine.

28. The media of claim 21, further comprising information that installs an actuator in the dynamic decoy system.

29. The media of claim 28, wherein the actuator at least one of executes the one or more portions of code, opens the one or more portions of code, inputs information to the one or more portions of code and simulates a passage of time longer than a period of testing.

30. The media of claim 21, wherein updating the dynamic decoy system is based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.